539,018

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

Rec'd PCT/PTO 16 JUN 2005

10/539018

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
8 juillet 2004 (08.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/057527 A1

(51) Classification internationale des brevets[7] : G06K 19/073

(21) Numéro de la demande internationale : PCT/FR2003/003773

(22) Date de dépôt international : 17 décembre 2003 (17.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/16084 18 décembre 2002 (18.12.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **OBERTHUR CARD SYSTEMS SA.** [FR/FR]; 102, Boulevard Malesherbes,, F-75017 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **GOUESSANT, Hervé** [FR/FR]; 25 impasse André Kommer,, F-94400 Vitry Sur Seine (FR). **JAYET, Stéphane** [FR/FR]; 85, rue des Charmettes,, F-69100 Villeurbanne (FR).

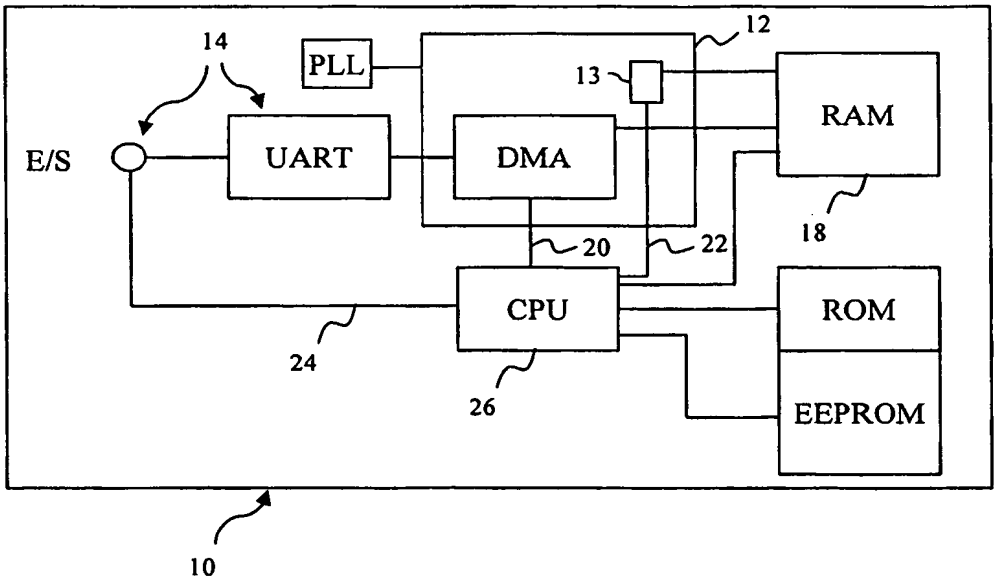
(74) Mandataire : **SANTARELLI**; 14, Avenue de la Grande-Armée, B.P. 237, Cedex 17, F-75822 Paris (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,

[Suite sur la page suivante]

(54) Title: OPTIMIZED DEVICE FOR DIGITAL DATA COMMUNICATION IN A MICROCIRCUIT CARD

(54) Titre : DSPOSITIF OPTIMISE DE COMMUNICATION DE DONNEES NUMERIQUES DANS UNE CARTE A MICROCIRCUIT



(57) **Abstract:** The invention concerns a microcircuit card comprising input/output means (14) for digital data, means for processing (12) said data and control means (26). The processing means (12) comprise means for transferring digital data (DMA) between the input/output means (14) and a storage zone (18), and means for communicating. with the control means (26), control data obtained at said digital data. The control means (26) control the transfer of the digital data by the transfer means (DMA) taking into account the control data.

[Suite sur la page suivante]

WO 2004/057527 A1

SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Cette carte à microcircuit comporte des moyens d'entrée-sortie (14) de données numériques, des moyens de traitement (12) de ces données et des moyens de contrôle (26). Les moyens de traitement (12) comportent des moyens de transfert (DMA) des données numériques entre les moyens d'entrée-sortie (14) et une zone de mémorisation (18), et des moyens de communication, avec les moyens de contrôle (26), de données de contrôle obtenues à partir desdites données numériques. Les moyens de contrôle (26) contrôlent le transfert des données numériques par les moyens de transfert (DMA) en prenant en compte les données de contrôle.

Dispositif optimisé de communication de données numériques dans une carte à microcircuit

La présente invention concerne une carte à microcircuit.

Plus précisément, l'invention vise une carte à microcircuit adaptée :

- d'une part à traiter un flux relativement important de données numériques échangées avec un dispositif extérieur à la carte ; et
- d'autre part à mettre en œuvre des procédures de sécurisation, par exemple des fonctions de vérification de l'intégrité des données numériques échangées avec le dispositif extérieur ou des fonctions cryptographiques d'authentification d'un utilisateur de la carte.

L'invention pourra ainsi être utilisée pour la décompression d'un flux de données numériques cryptées.

Selon une architecture connue d'une telle carte, les données numériques reçues depuis un port d'entrée-sortie de la carte à microcircuit sont lues par un microprocesseur et traitées au fil de leur réception. Le microprocesseur effectue les contrôles de sécurité précités au fur et à mesure qu'il reçoit les données numériques.

Un problème majeur de cette architecture est que le flux de données numériques pouvant être échangées par la carte est limité par la fréquence du microprocesseur (généralement de l'ordre de 4 MHz pour les cartes à microcircuit connues de l'état de la technique).

Dans d'autres domaines de l'électronique, pour palier les limites associées à la fréquence d'un microprocesseur, le transfert de données à haut débit est souvent réalisé par des composants dédiés appelés DMA (Direct Memory Access). Ces composants DMA sont programmés par un microprocesseur pour effectuer un transfert prédéterminé, par exemple entre un port d'entrée-sortie et une mémoire, le transfert en tant que tel n'étant pas réalisé par le microprocesseur.

Malheureusement, ces composants DMA sont dédiés au transfert de données et ne permettent pas d'effectuer de traitement sur les données au cours

données sensibles nécessitant des opérations de sécurisation, comme c'est le cas pour les cartes à microcircuit précitées.

L'invention vise, en surmontant cette apparente incompatibilité, à permettre un transfert d'un flux important ou rapide de données sécurisées dans une carte à microcircuit tout en maintenant un niveau de sécurité important, ce grâce à une association originale d'un processeur et d'un DMA.

Elle propose à cet effet une carte à microcircuit comportant :

- des moyens d'entrée-sortie de données numériques;
- des moyens de traitement de ces données ; et
- des moyens de contrôle de flux.

La carte à microcircuit est caractérisée en ce que les moyens de traitement comportent :

- des moyens de transfert de ces données numériques entre les moyens d'entrée-sortie et une zone de mémorisation ; et
- des moyens de communication, avec les moyens de contrôle de flux, de données de sécurisation obtenues à partir des données numériques, les moyens de contrôle de flux étant adaptés à contrôler le transfert des données numériques par les moyens de transfert en prenant en compte ces données de sécurisation.

Ainsi, les données reçues depuis le port de communication sont transférées par les moyens de transfert vers une zone de mémorisation, le flux de ce transfert n'étant pas limité par la vitesse des moyens de contrôle de flux.

Par ailleurs, au cours de ce transfert, des données de sécurisation obtenues à partir des données numériques sont communiquées par les moyens de traitement aux moyens de contrôle de flux, le flux de ces données de sécurisation reçues par les moyens de contrôle de flux étant limité et de toutes façons bien inférieur au flux de données numériques reçues par la carte.

Les moyens de contrôle de flux, constitués par exemple par un processeur, sont alors à même d'effectuer, en utilisant ces données de sécurisation, les opérations nécessaires de contrôle des moyens de transfert pour garantir le respect des contraintes de sécurité.

L'invention permet ainsi d'augmenter le flux de données numériques traitées par la carte à microcircuit, tout en maintenant le niveau de sécurité d'une carte traditionnelle.

Dans une première variante de réalisation de la carte à microcircuit selon l'invention, les données de sécurisation précitées sont constituées, au moins en partie, par une partie des données numériques transférées par la carte.

Dans un mode préféré de cette première variante de réalisation, les données de sécurisation comportent des données d'authentification d'une partie des données numériques reçues par la carte, les moyens de contrôle de flux étant adaptés à vérifier la validité des données numériques à partir de ces données d'authentification, et à contrôler le transfert en fonction du résultat de cette vérification.

De façon connue, lorsque la carte reçoit des données numériques transmises par un dispositif extérieur, si les moyens de contrôle de flux déterminent que les données d'authentification ne sont pas valides, cela signifie que les données numériques n'ont pas été envoyées par un émetteur autorisé.

Dans ce cas, les moyens de contrôle de flux peuvent prendre une mesure prédéterminée, telle que bloquer l'utilisation de la carte ou envoyer un message d'erreur.

Dans un mode préféré de réalisation, afin de garantir une utilisation sécurisée de la carte, les moyens de contrôle de flux commandent l'arrêt du transfert des données numériques par les moyens de transfert lorsque les données d'authentification ne sont pas valides.

La carte peut ainsi recevoir un flux important de données, une partie seulement de ces données étant communiquée aux moyens de contrôle de flux pour garantir la sécurité exigée.

Dans une deuxième variante de réalisation, les moyens de traitement sont adaptés à insérer dans les données de sécurisation un résultat de traitement calculé à partir des données numériques.

Le résultat de traitement peut par exemple être le résultat d'une étape de vérification des données d'authentification précitées par des moyens de calcul compris dans les moyens de traitement, par exemple des moyens cryptographiques de la carte à microcircuit. Ce résultat est ensuite pris en

compte par les moyens de contrôle de flux pour vérifier l'intégrité des données numériques et pour contrôler leur transfert par les moyens de transfert en conséquence.

Cette étape d'authentification peut consister à vérifier une signature, par exemple en utilisant une clef cryptographique et une fonction de hachage selon un algorithme du type MD4, MD5 ou SHA-1.

Dans cette variante, ce sont les moyens de contrôle de flux qui effectuent les étapes de vérification des données d'authentification. Ils peuvent ensuite prendre une mesure prédéterminée telle qu'arrêter le transfert des données numériques ou bloquer l'utilisation de la carte, en cas d'utilisation frauduleuse de celle-ci.

Dans un mode de réalisation préféré, les moyens de contrôle de flux effectuent le contrôle du transfert des données numériques en modifiant au moins un paramètre de fonctionnement des moyens de transfert.

Par exemple, ce paramètre de fonctionnement est une adresse de mémorisation des données numériques dans la zone de mémorisation.

Ainsi, lorsque le taux d'occupation d'une première plage de la zone de mémorisation est supérieur à un seuil prédéterminé, les moyens de contrôle de flux peuvent paramétrer les moyens de transfert pour que les données numériques reçues par les moyens de transfert soient mémorisées à cette adresse.

Le paramètre précité peut également être un paramètre permettant de sélectionner le protocole de communication entre les moyens d'entrée-sortie et la zone de mémorisation. Ce protocole de communication peut par exemple être adapté aux transferts de données sécurisées.

Selon différentes variantes de réalisation de la carte à microcircuit selon l'invention, les moyens de traitement comportent une unité de compression des données, une unité de décompression des données, une unité de cryptage des données ou une unité de décryptage des données.

Dans une autre variante de réalisation, les moyens de contrôle de flux sont en outre adaptés à obtenir des données préliminaires directement à partir des moyens d'entrée-sortie, les données préliminaires étant prises en compte

par l'unité de contrôle de flux pour autoriser ou refuser le transfert des données numériques par les moyens de transfert.

Dans un mode particulier de cette variante de réalisation, ces données préliminaires comportent des données d'authentification.

Ce mode de réalisation permet d'obtenir un niveau de sécurité supplémentaire, par exemple par le contrôle d'un code d'authentification, préalablement au transfert des données numériques proprement dites. Contrairement aux données de sécurité, ce code d'authentification n'est typiquement vérifié qu'une seule fois en début de session de transfert. Il peut demander plus de temps calcul, et donc mettre en œuvre un algorithme d'authentification complexe et permettant d'obtenir un niveau de sécurité renforcé.

Dans un autre mode de réalisation préféré, ces données préliminaires comportent une adresse de mémorisation des données numériques qui seront transférées par les moyens de transfert. Dans ce mode de réalisation préféré, ces données préliminaires peuvent en outre comporter des données d'authentification de cette adresse de mémorisation, ceci afin de garantir que l'adresse de mémorisation n'a pas été fournie par un utilisateur non autorisé.

Selon un mode de réalisation particulièrement avantageux, la carte à microcircuit comporte en outre des moyens de régulation adaptés à modifier une fréquence d'horloge appliquée aux moyens de traitement en fonction desdites données de sécurisation.

Cette caractéristique permet ainsi de limiter la consommation électrique de la carte à microcircuit lorsque le transfert de données numériques par les moyens de transfert doit être interrompu.

L'invention sera mieux comprise et d'autres avantages apparaîtront plus clairement à la lumière de la description qui va suivre d'une carte à microcircuit conforme à son principe, donnée uniquement à titre d'exemple et faite en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma bloc d'une carte à microcircuit conforme à la technique antérieure ;
- la figure 2 est un schéma bloc analogue à la figure 1 illustrant un mode de réalisation possible d'une carte à microcircuit conforme à l'invention ; et

- la figure 3 est un exemple de données de sécurisation conformément à l'invention.

La carte à microcircuit 10 conforme à l'art antérieur représentée sur la figure 1 comporte principalement un processeur CPU associé de façon classique à un certain nombre de mémoires (du type RAM, ROM, EEPROM), des moyens de traitement 12 et des moyens d'entrée-sortie 14 reliés par exemple, à un terminal.

Les moyens de traitement 12 comportent une unité de calcul 13 adaptée à réaliser le traitement proprement dit des données numériques, à savoir par exemple des opérations de compression, de décompression, de cryptage ou de décryptage de ces données.

Dans un mode de réalisation préféré, les moyens d'entrée-sortie 14 permettant à la carte à microcircuit 10 de communiquer avec un terminal ou une entité électronique extérieure, comprennent essentiellement une unité d'émission réception asynchrone de type UART.

Les moyens d'entrée-sortie 14 peuvent aussi être adaptés à mettre en œuvre des protocoles de communication standardisés et connus de l'homme du métier, à savoir par exemple, les protocoles connus sous les références "T=0", "T=1" (ISO 7816), USB, FireWire ou I2C.

Selon l'art antérieur, lorsque la carte à microcircuit 10 reçoit via l'UART des données numériques qui doivent être soumises à un traitement par l'unité de calcul 13 des moyens de traitement 12, l'UART transmet un message d'interruption au processeur CPU. Le processeur CPU vient alors lire un registre de l'UART et copier les données dans la mémoire RAM.

Le processeur CPU initialise alors les moyens de traitement 12 puis va lire les données à traiter dans la mémoire RAM et les copie dans un registre 16 des moyens de traitement 12.

Afin d'être communiqué au terminal extérieur, le résultat calculé par les moyens de traitement 12 est ensuite lu par le processeur CPU dans le registre 16 et copié dans le registre UART par le processeur CPU.

Un tel mode de fonctionnement n'est pas favorable au traitement de données numériques à haut débit par la carte à microcircuit 10. En effet, l'opération intermédiaire réalisée par le processeur CPU de copie des données

numériques dans la zone de mémorisation RAM avant traitement par les moyens de traitement 12 est tout particulièrement pénalisante.

Or, on souhaite augmenter la puissance de traitement d'une telle carte à microcircuit pour traiter des flux importants et continus de données en temps réel.

A titre d'exemple, on souhaite pouvoir procéder au déchiffrement en temps réel de données numériques représentatives d'un son. De telles données sont compressées selon la norme MP3 et transmises à une vitesse de 128 kbits/s. La carte à microcircuit chargée du déchiffrement en temps réel nécessite donc de pouvoir recevoir et traiter des informations à haut débit.

Une carte à microcircuit conforme à l'invention et permettant de résoudre le problème précédent va maintenant être décrite en référence à la figure 2.

Conformément à la présente invention, les moyens de traitement 12 comportent des moyens de transfert DMA des données numériques entre le port de communication 14 et une zone de mémorisation 18.

Dans l'exemple de la figure 2 décrit ici, la zone de mémorisation 18 est une mémoire vive RAM.

Dans d'autres modes de réalisation, la zone de mémorisation 18 peut être choisie parmi différents types de mémoires réinscriptiples, à savoir par exemple, une mémoire Flash, une mémoire de type EEPROM ou un disque dur.

Dans une autre variante de réalisation, la zone de mémorisation 18 est un port de l'unité de calcul 13 des moyens de traitement 12.

Dans le mode de réalisation préféré décrit ici, ces moyens de transfert DMA comportent un composant électronique dédié connu de l'homme du métier appelé DMA (Direct Memory Access).

De façon connue, de tels composants se programment par l'écriture de paramètres dans des registres de configuration.

A titre d'exemple non limitatif, de tels paramètres comportent l'adresse d'un port des moyens d'entrée-sortie 14, l'adresse d'une plage de la zone de mémorisation 18 dans laquelle les données numériques doivent être mémorisées, et des paramètres représentatifs d'un critère d'arrêt du transfert.

Quoiqu'il en soit, la carte à microcircuit selon l'invention comporte en outre des moyens de contrôle de flux 26 adaptés à contrôler le transfert des données numériques par les moyens de transfert DMA.

En particulier, lorsque les données numériques doivent être transférées vers une zone de mémorisation 18 de type EEPROM, les moyens de contrôle de flux 26 sont adaptés à contrôler un générateur de tension ou tout autre moyen permettant d'appliquer une tension électrique suffisante à la mémoire EEPROM pour que celle ci soit accessible en écriture.

Dans le mode de réalisation décrit en référence à la figure 2, les moyens de contrôle de flux 26 sont constitués par un processeur CPU, lequel est classiquement associé à ces différentes mémoires (RAM, ROM, EEPROM) comme dans le cas de la figure 1.

Le paramétrage des moyens de transfert DMA par les moyens de contrôle de flux 26 est représenté schématiquement par les signaux 20 à la figure 2.

Conformément à la présente invention, les moyens de traitement 12 comportent également des moyens de communication 22 entre son unité de calcul 13 et les moyens de contrôle de flux 26.

Ces moyens de communication 22 permettent l'échange de données de sécurisation entre les moyens de traitement 12 et les moyens de contrôle de flux 26, ces données de sécurisation étant obtenues à partir des données numériques DATA transférées par les moyens de transfert DMA.

Chronologiquement, une fois les moyens de transfert DMA programmés par les moyens de contrôle de flux 26 au moyen des signaux 20, les moyens de transfert DMA réalisent le transfert des données numériques entre les moyens d'entrée-sortie 14 et la zone de mémorisation 18. L'unité de calcul 13 des moyens de traitement 12 obtient ensuite les données de sécurisation DATA_CTRL à partir des données numériques DATA mémorisées dans la zone de mémorisation 18 et les communique aux moyens de contrôle de flux 26 par les moyens de communication 22.

Un exemple de données de sécurisation DATA_CTRL, dans un mode préféré de réalisation, est donné à la figure 3.

Les données de sécurisation DATA_CTRL comportent une partie P1 des données numériques et des données d'authentification AUTH calculées à partir des données numériques de la partie P1.

Dans une première variante de réalisation, les données d'authentification AUTH forment une signature de P1. Typiquement, il s'agit des données P1 auxquelles on a appliquées, une fonction de Hachage connue tel que MD4, MD5 ou SHA-1, puis un algorithme de cryptage. Pour cela, on peut utiliser un algorithme de cryptage à clef symétrique tel que l'algorithme DES (Data Encryption Standard) ou un algorithme à clef asymétrique tel que l'algorithme RSA (du nom de ses inventeurs Rivest, Shamir et Adelman).

Dans cette variante, sur réception de ces données de sécurisation DATA_CTRL, les moyens de contrôle de flux 26 décryptent tout d'abord la signature AUTH avec la clef de décryptage et obtiennent un premier résultat HASH1. Les moyens de contrôle de flux 26 appliquent ensuite la fonction de hachage à la partie P1 et obtiennent un deuxième résultat HASH2.

Les moyens de contrôle de flux 26 comparent ensuite le premier résultat HASH1 et deuxième résultat HASH2.

Dans un mode de réalisation préféré de cette première variante, lorsque ces résultats HASH1 et HASH2 diffèrent, les moyens de contrôle de flux 26 commandent l'arrêt du transfert des données numériques par l'envoi d'un signal d'arrêt.

Dans le mode de réalisation préféré, les moyens de traitement 12 insèrent dans les données de sécurisation DATA_CTRL un résultat de traitement des données numériques DATA par l'unité de calcul 13.

Ce résultat de traitement est par exemple l'adresse à laquelle une partie des données numériques DATA a été mémorisée par les moyens de transfert DMA dans la zone de mémorisation 18, les moyens de contrôle de flux 26 étant alors adaptés à lire les données de cette partie, à en vérifier la validité, et à contrôler le transfert des données numériques DATA par les moyens de transfert DMA en fonction du résultat de cette vérification.

Dans un mode de réalisation dans lequel les moyens de traitement 12 comportent des moyens cryptographiques 13, ce résultat de traitement est le

résultat, obtenu par l'unité cryptographique 13, d'une étape d'authentification des données numériques DATA.

En variante, le résultat de traitement est le résultat, obtenu par les moyens cryptographiques 13, d'une étape de vérification d'une signature des données numériques DATA.

Cette étape de vérification peut par exemple être le décryptage des données AUTH,ce décryptage étant réalisé en utilisant un algorithme RSA pour obtenir un résultat similaire au premier résultat HASH1.

Dans un mode de réalisation préféré, les moyens de contrôle de flux 26 sont en outre adaptés à obtenir des données préliminaires directement à partir des moyens d'entrée-sortie 14, par le chemin de données 24 représenté à la figure 2.

En variante, les données préliminaires sont obtenues par les moyens de contrôle de flux 26 à partir d'un deuxième port d'entrée-sortie, par exemple en utilisant le protocole connu sous la référence "T=0" (ISO 7816), les moyens d'entrée-sortie 14 étant réservés au transfert des données numériques DATA par les moyens de transfert DMA.

Le chemin de données 24 peut également être un chemin de données bidirectionnel utilisé par les moyens de contrôle de flux 26 pour communiquer des informations à un dispositif extérieur à la carte à microcircuit. Ces informations peuvent par exemple être constituées par un message d'erreur émis par les moyens de contrôle de flux 26 lorsque ceux-ci détectent, à partir des informations de sécurisation, la présence de données numériques erronées.

Ces informations peuvent également être constituées par un flux de données sortant de la carte à microcircuit, ce flux de données étant le résultat du traitement, par les moyens de traitement 12, des données numériques DATA reçues par la carte.

Ces données préliminaires comportent par exemple des données d'authentification PASSWD, ces données préliminaires étant quoi qu'il en soit prises en compte pour contrôler le transfert des données numériques par les moyens de transfert DMA.

Ainsi, par exemple si les données d'authentification PASSWD ne sont pas conformes à une règle de contrôle prédéterminée, cette règle pouvant être

mémorisée dans la mémoire ROM, les moyens de contrôle de flux 26 ne programment pas les moyens de transfert DMA pour réaliser le transfert de données numériques entre les moyens d'entrée-sortie 14 et la zone de mémorisation 18.

Préférentiellement, les données préliminaires comportent une adresse de mémorisation des données numériques.

Dans une variante de réalisation, la carte à microcircuit comporte des moyens de régulation PLL adaptés à modifier une fréquence d'horloge appliquée aux moyens de traitement 12 en fonction des données de contrôle DATA_CTRL.

Ces moyens de régulation PLL peuvent par exemple être constitués par un composant de type PLL (Phase Lock Looping en anglais) connu de l'homme du métier et permettant de dériver des signaux de différentes fréquences d'horloge, à partir d'un signal d'une horloge externe non représentée.

Dans le mode préféré de réalisation ces moyens de régulation PLL sont commandés par les moyens de contrôle de flux 26 afin d'ajuster la consommation électrique des moyens de traitement 12 en fonction du flux de données numériques DATA.

Selon le mode de réalisation choisi, les moyens de transfert DMA peuvent être unidirectionnels ou bidirectionnels. L'invention s'applique en particulier pour contrôler le transfert de données numériques cryptées DATA à partir de la zone de mémorisation 18 vers les moyens d'entrée-sortie 14.

REVENDICATIONS

1. Carte à microcircuit comportant :
   - des moyens d'entrée-sortie (14) de données numériques (DATA);
   - des moyens de traitement (12) de ces données ; et
   - des moyens de contrôle de flux (26),

la carte à microcircuit étant caractérisée en ce que les moyens de traitement (12) comportent :

- des moyens de transfert (DMA) desdites données numériques (DATA) entre les moyens d'entrée-sortie (14) et une zone de mémorisation (18); et

- des moyens de communication (20), avec les moyens de contrôle de flux (26), de données de sécurisation (DATA_CTRL) obtenues à partir desdites données numériques (DATA),

les moyens de contrôle de flux (26) étant adaptés à contrôler le transfert des données numériques (DATA) par les moyens de transfert (DMA) en prenant en compte lesdites données de sécurisation (DATA_CTRL).

2. Carte à microcircuit selon la revendication 1, caractérisée en ce que lesdites données de sécurisation (DATA_CTRL) sont constituées au moins en partie par une partie desdites données numériques (DATA).

3. Carte à microcircuit selon la revendication 2, caractérisée en ce que lesdites données de sécurisation (DATA_CTRL) comportent des données d'authentification (AUTH) d'une partie (P1) des données numériques reçues par la carte, les moyens de contrôle de flux (26) étant adaptés à vérifier la validité desdites données numériques (DATA) à partir de ces données d'authentification (AUTH) et à contrôler ledit transfert en fonction du résultat de cette vérification.

4. Carte à microcircuit selon l'une quelconque des revendications 1 à 3, caractérisée en ce que lesdits moyens de traitement (12) sont adaptés à insérer dans lesdites données de sécurisation (DATA_CTRL), un résultat de traitement desdites données numériques (DATA).

5. Carte à microcircuit selon la revendication 4 caractérisée en ce que ledit résultat de traitement est le résultat d'une étape d'authentification desdites données numériques.

6. Carte à microcircuit selon l'une quelconque des revendications 1 à 5, caractérisée en ce que les moyens de contrôle de flux sont adaptés à modifier au moins un paramètre de fonctionnement desdits moyens de transfert (DMA).

7. Carte à microcircuit selon la revendication 6 caractérisée en ce que ledit paramètre est choisi parmi une adresse de ladite zone de mémorisation (18) et un paramètre de sélection d'un protocole de communication entre les moyens d'entrée-sortie (14) et la zone de mémorisation (18).

8. Carte à microcircuit selon l'une quelconque des revendications 1 à 7, caractérisée en ce que lesdits moyens de traitement (12) comportent une unité (13) de compression de données, une unité de décompression de données, une unité de cryptage de données, ou une unité de décryptage de données.

9. Carte à microcircuit selon l'une quelconque des revendications 1 à 8, caractérisée en ce que lesdits moyens de contrôle de flux (26) sont adaptés à arrêter le transfert des données numériques (DATA) par lesdits moyens de transfert (DMA) lorsqu'ils détectent, à partir desdites données de sécurisation (DATA_CTRL), la présence de données d'authentification invalides parmi lesdites données numériques (DATA).

10. Carte à microcircuit selon l'une quelconque des revendications 1 à 9 caractérisée en ce que les moyens de contrôle de flux (26) sont en outre adaptés à obtenir des données préliminaires directement à partir des moyens d'entrée-sortie (14), les données préliminaires étant également prises en compte par les moyens de contrôle de flux (26) pour autoriser ou refuser le transfert des données numériques (DATA) par les moyens de transfert (DMA).

11. Carte à microcircuit selon la revendication 10, caractérisée en ce que lesdites données préliminaires comportent des données d'authentification (PASSWD) .

12. Carte à microcircuit selon la revendication 10 ou 11, caractérisée en ce que lesdites données comportent une adresse de mémorisation desdites données numériques.

13. Carte à microcircuit selon l'une quelconque des revendications 1 à 12, caractérisée en ce qu'elle comporte en outre des moyens de régulation (PLL) adaptés à modifier une fréquence d'horloge appliquée aux moyens de traitement (12) en fonction desdites données de sécurisation (DATA_CTRL).

14. Carte à microcircuit selon l'une quelconque des revendications 1 à 13, caractérisée en ce que lesdits moyens de transfert (DMA) comportent un composant DMA.

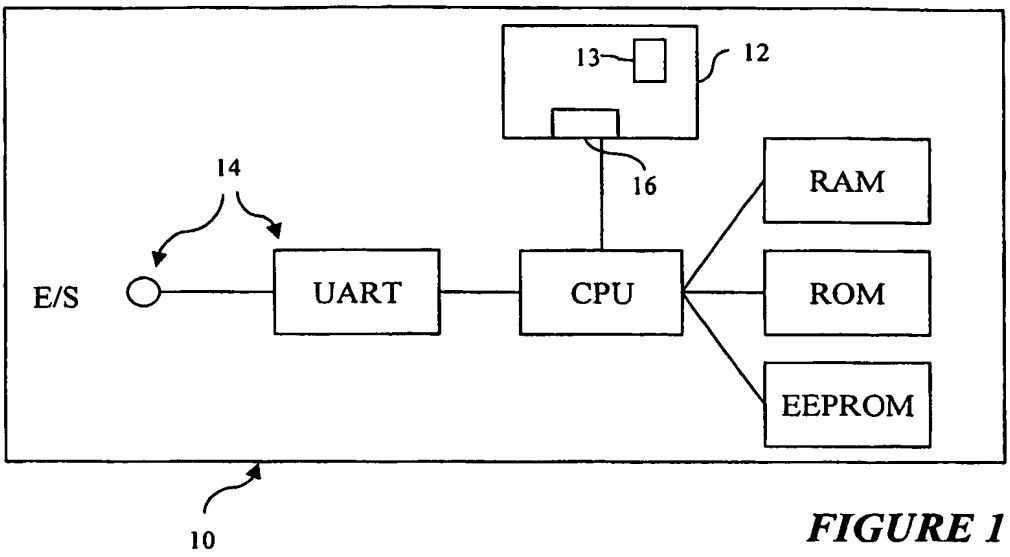


FIGURE 1

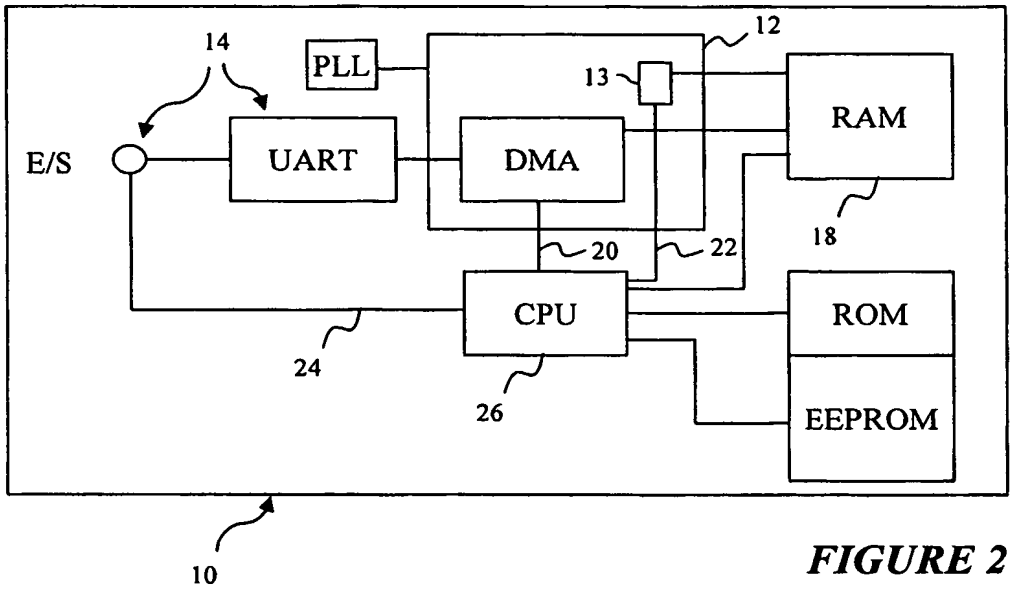


FIGURE 2

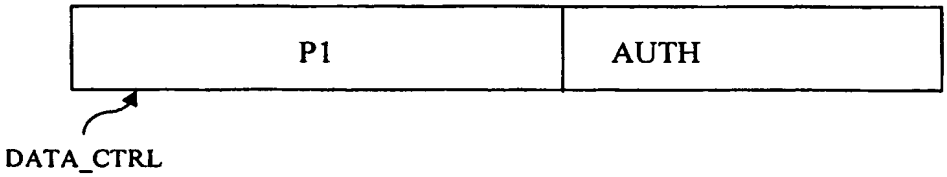


FIGURE 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT 03/03773

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 199 08 285 A (ORGA KARTENSYSTEME GMBH) 31 August 2000 (2000-08-31) column 2, line 16 - line 32; figure 1	1,6,10, 11
X	EP 0 552 079 A (GEMPLUS CARD INT) 21 July 1993 (1993-07-21) column 3, line 57 -column 4, line 49 column 6, line 5 - line 17 column 6, line 46 -column 7, line 4 column 8, line 7 - line 31 column 9, line 27 - line 42 column 10, line 1 - line 17	1-3,6-11
Y		14,15
Y	FR 2 783 336 A (SCHLUMBERGER IND SA) 17 March 2000 (2000-03-17) page 6, line 17 -page 7, line 11	14

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 May 2004	03/06/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bhalodia, A

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

[redacted]

International Application No
P[redacted]R 03/03773

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 787 101 A (KELLY MICHAEL GENE) 28 July 1998 (1998-07-28) abstract	15
A	-----	1-14

INTERNATIONAL SEARCH REPORT

[redacted]ion on patent family members

[redacted]al Application No
PCT[redacted] 03/03773

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19908285 A	31-08-2000	DE 19908285 A1	31-08-2000
		AT 257258 T	15-01-2004
		AU 3271200 A	21-09-2000
		WO 0052635 A1	08-09-2000
		DE 50004926 D1	05-02-2004
		EP 1163634 A1	19-12-2001
EP 0552079 A	21-07-1993	FR 2686170 A1	16-07-1993
		DE 69327181 D1	13-01-2000
		DE 69327181 T2	15-06-2000
		EP 0552079 A1	21-07-1993
		ES 2142337 T3	16-04-2000
		JP 5314013 A	26-11-1993
		SG 52681 A1	28-09-1998
		US 6182205 B1	30-01-2001
		US 5875480 A	23-02-1999
FR 2783336 A	17-03-2000	FR 2783336 A1	17-03-2000
		AT 255256 T	15-12-2003
		CN 1317123 T	10-10-2001
		DE 69913166 D1	08-01-2004
		DK 1110173 T3	05-04-2004
		EP 1110173 A1	27-06-2001
		WO 0016255 A1	23-03-2000
		JP 2002525720 T	13-08-2002
US 5787101 A	28-07-1998	AU 684184 B2	04-12-1997
		AU 2606395 A	05-01-1996
		BR 9507981 A	12-08-1997
		CA 2191555 A1	21-12-1995
		CN 1150846 A ,B	28-05-1997
		DE 69508082 D1	08-04-1999
		DE 69508082 T2	24-06-1999
		DK 765501 T3	27-09-1999
		EP 0765501 A1	02-04-1997
		ES 2128060 T3	01-05-1999
		FI 965018 A	13-12-1996
		JP 10501910 T	17-02-1998
		NO 965331 A	12-12-1996
		WO 9534863 A1	21-12-1995

RAPPORT DE RECHERCHE INTERNATIONALE

[redacted] internationale No
PCT/[redacted] 03/03773

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06K19/073

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	DE 199 08 285 A (ORGA KARTENSYSTEME GMBH) 31 août 2000 (2000-08-31) colonne 2, ligne 16 - ligne 32; figure 1 ---	1,6,10, 11
X	EP 0 552 079 A (GEMPLUS CARD INT) 21 juillet 1993 (1993-07-21) colonne 3, ligne 57 -colonne 4, ligne 49 colonne 6, ligne 5 - ligne 17 colonne 6, ligne 46 -colonne 7, ligne 4 colonne 8, ligne 7 - ligne 31 colonne 9, ligne 27 - ligne 42 colonne 10, ligne 1 - ligne 17	1-3,6-11
Y	 ---	14,15
Y	FR 2 783 336 A (SCHLUMBERGER IND SA) 17 mars 2000 (2000-03-17) page 6, ligne 17 -page 7, ligne 11 ---	14
	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
4 mai 2004	03/06/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bhalodia, A

RAPPORT DE RECHERCHE INTERNATIONALE

[redacted] Internationale No
PCT/[redacted] 03/03773

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 5 787 101 A (KELLY MICHAEL GENE) 28 juillet 1998 (1998-07-28) abrégé	15
A	-----	1-14

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements rel [redacted] res de familles de brevets

[redacted] nternationale No
PC[redacted] 03/03773

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
DE 19908285	A	31-08-2000	DE	19908285 A1	31-08-2000
			AT	257258 T	15-01-2004
			AU	3271200 A	21-09-2000
			WO	0052635 A1	08-09-2000
			DE	50004926 D1	05-02-2004
			EP	1163634 A1	19-12-2001
EP 0552079	A	21-07-1993	FR	2686170 A1	16-07-1993
			DE	69327181 D1	13-01-2000
			DE	69327181 T2	15-06-2000
			EP	0552079 A1	21-07-1993
			ES	2142337 T3	16-04-2000
			JP	5314013 A	26-11-1993
			SG	52681 A1	28-09-1998
			US	6182205 B1	30-01-2001
			US	5875480 A	23-02-1999
FR 2783336	A	17-03-2000	FR	2783336 A1	17-03-2000
			AT	255256 T	15-12-2003
			CN	1317123 T	10-10-2001
			DE	69913166 D1	08-01-2004
			DK	1110173 T3	05-04-2004
			EP	1110173 A1	27-06-2001
			WO	0016255 A1	23-03-2000
			JP	2002525720 T	13-08-2002
US 5787101	A	28-07-1998	AU	684184 B2	04-12-1997
			AU	2606395 A	05-01-1996
			BR	9507981 A	12-08-1997
			CA	2191555 A1	21-12-1995
			CN	1150846 A ,B	28-05-1997
			DE	69508082 D1	08-04-1999
			DE	69508082 T2	24-06-1999
			DK	765501 T3	27-09-1999
			EP	0765501 A1	02-04-1997
			ES	2128060 T3	01-05-1999
			FI	965018 A	13-12-1996
			JP	10501910 T	17-02-1998
			NO	965331 A	12-12-1996
			WO	9534863 A1	21-12-1995